UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	Criminal No. 20-40036-TSH
VINCENT KIEJZO,	)	
	)	
	)	
Defendant	)	
	)	
	)	

ORDER ON MOTION FOR DISCOVERY

October 4, 2021

Hennessy, M.J.

Defendant is charged by indictment with one count of Possession of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). He has moved to compel discovery which the parties briefed and argued at an in-person hearing. For the reasons that follow, the motion is denied.

I. Factual and Procedural Background

On September 8, 2020, DHS special agent Caitlin Moynihan applied for a warrant for Defendant's residence. [Dkt. No. 2-3]. Her supporting affidavit alleged probable cause to believe that a computer in Defendant's home accessed two child pornography websites, Website 2 and Website 3, operating on the TOR network. [Dkt. No. 80-6, ¶ 5]. Among other averments, Moynihan presented information about the content of Websites 2 and 3, including detailed descriptions of images of child pornography found there, topics available to users, and user posts. [Id. ¶¶ 15–29]. Moynihan averred that the TOR network, on which these websites operated, is designed to anonymize the IP addresses which access TOR network websites by routing internet

communications through a path of random IP addresses before reaching a destination computer, as well as the IP addresses hosting services on the TOR network that users may access. [Id., ¶¶ 7–8, 14]. Moynihan noted that hidden service websites on the TOR network are not indexed or easily identified by search engines, such as Google, and generally a user would need to take deliberate steps to access Website 2 or Website 3, including knowing and inputting the 16 or 56-character web address for either. [Id. ¶ 35]. Thus, while the TOR network does not guarantee anonymity for a user accessing its hidden services, the routing of communications through a path of IP addresses makes traditional identification techniques largely ineffective. [Id. ¶¶ 7, 11]. Given the anonymity the TOR network creates, and that TOR hidden service websites are accessible to users anywhere in the world, it is common for law enforcement agencies from investigating countries to share information relevant to an offender or a site in other countries. [Id. ¶ 35].

According to Moynihan, in June 2019 a foreign law enforcement agency ("FLA") seized the computer server(s) located outside the U.S. which hosted Website 2 and Website 3. [Id. ¶¶ 15, 23]. In August 2019, an FLA "known to U.S. law enforcement and with a history of providing reliable, accurate information" notified U.S. law enforcement that it had determined that IP address 96.230.213.63 (the "96 IP address") had accessed Website 2 on May 12, 2019 at a certain time, and Website 3 on the same date about 16 minutes thereafter. [Id. ¶¶ 31–32].[1] Moynihan averred the notifying FLA was "a national law enforcement agency of a country with an established rule of law;" that the FLA and U.S. law enforcement had a long history of criminal information-sharing; that the notifying "FLA advised U.S. law enforcement that it had obtained [the IP] information through independent investigation that was lawfully authorized in the FLA's country pursuant to

[1] The Government disclosed in discovery that the notifying FLA, the [redacted], was not the seizing FLA. [Dkt. No. 80, p. 1 n.1].

its national laws;" that in doing so the "FLA had not interfered with, accessed, searched, or seized any data from any computer in the [U.S.] in order to obtain the IP address information;" and that U.S. law enforcement "did not participate in the investigative work through which the FLA identified the IP address." [Id. ¶ 33]. Moynihan recounted that prior tips associated with TOR network child exploitation websites from the notifying FLA led to the identification and arrest of a U.S.-based producer of child pornography and hands-on offender, and rescue of child victims of this offender; the seizure of evidence of child pornography trafficking and possession; and corroboration for information independently developed of child pornography trafficking and possession. [Id. ¶ 34].

On March 20, 2020, agents issued an administrative subpoena to Verizon Fios for customer information for the user of the 96 IP address on the date and times provided in the tip. [Id. ¶ 39]. Verizon reported the 96 IP address belonged to Defendant's residence. [Id.]. Agents executed the warrant on September 9, 2020. [Dkt. No. 2-3, ¶ 5]. In Defendant's bedroom, agents located a thumb drive which contained 6,000 video files, including files depicting minors engaged in sexually explicit conduct, and a document with four links to the TOR network. [Id. ¶¶ 9–10]. Defendant was present, waived his Miranda rights, and when informed of what agents had located admitted possessing child pornography on the thumb drive and accessing the TOR network. [Id. ¶¶ 12–13].

Following indictment and the Government's discovery production, Defendant requested additional discovery, some of which the Government provided. As noted, during discovery, the Government advised Defendant that the FLA which seized the servers hosting Websites 2 and 3 was not the notifying FLA [redacted] [Dkt. No. 80, p. 1 n.1]. Defendant then moved to compel discovery and for an in-person hearing on the motion. Defendant alleged that the discovery he

sought to compel was required under Fed. R. Crim. P. 16, Local Rules 116.1 and 116.2, Brady v. Maryland, 373 U.S. 83 (1963), the Fifth Amendment, and Defendant's ability to prosecute a hearing pursuant to Franks v. Delaware, 438 U.S. 154 (1978). [Dkt. No. 80].

II. Legal Standard

Rule 16 of the Federal Rules of Criminal Procedure directs the government, upon a defendant's request, to allow a defendant to inspect and copy any item in the government's possession, custody, or control that is either (i) material to preparing the defense; (ii) an item the government intends to use in its case-in-chief at trial; or (iii) was obtained from or belongs to the defendant. See Fed. R. Crim. P. 16(a)(1)(E). As to the first category, a defendant, as the moving party, bears the burden of showing materiality. United States v. Goris, 876 F.3d 40, 44 (1st Cir. 2017). "A showing of materiality requires 'some indication' that the pretrial disclosure of the information sought 'would have enabled the defendant significantly to alter the quantum of proof in his favor.'" Id. (quoting United States v. Ross, 511 F.2d 757, 763 (5th Cir. 1975)). A significant alteration may occur in myriad ways, including "uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." Id. (quoting United States v. Lloyd, 992 F.2d 348, 351 (D.C. Cir. 1993)). However, a showing that what is sought bears some abstract relationship to the issues in the case is not enough. Id.

Local Rule 116.1 does not add much for purposes of this motion; it requires the government to produce all information to which a defendant is entitled under Rule 16. See Local Rule 116.1(c)(1)(A). In relevant part, Local Rule 116.2 implements Brady v. Maryland, 373 U.S. 83 (1963) and its progeny, and defines exculpatory evidence to include information which tends to cast doubt on: a defendant's guilt or any essential element of a charged offense; the admissibility of evidence that the government may offer in its case-in-chief; the credibility or accuracy of

evidence the government may offer in its case-in-chief; or information that tends to diminish a defendant's culpability. See Local Rule 116.2(a).

Finally, Defendant claims the discovery is needed for him to prosecute a Franks hearing. In Franks v. Delaware, the Court said:

> There is, of course, a presumption of validity with respect to the affidavit supporting the search warrant. To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. . . . The deliberate falsity or reckless disregard whose impeachment is permitted today is only that of the affiant, not of any nongovernmental informant.

438 U.S. at 171. Entitlement to discovery to mount a Franks challenge requires the same substantial preliminary showing. See United States v. Long, 774 F.3d 653, 661–62 (10th Cir. 2014) (disclosure of informant not required where defendant's allegations consisted solely of speculation and failed to make the substantial preliminary showing required by Franks); United States v. Messalas, 17-cr-339 (RRM), 2020 WL 1666162, at *11 (E.D.N.Y. Apr. 4, 2020) ("Messalas cannot seek discovery to support his Franks challenge without first making the preliminary showing required to grant a Franks hearing"); United States v. Harding, 273 F. Supp. 2d 411, 430 (S.D.N.Y. 2003) (where defendant failed to make the substantial preliminary showing for a Franks hearing, he is not entitled to "wide-ranging discovery to canvass for evidence to support his motion to suppress."); cf. United States v. Koschtschuk, 09-cr-0096(S)(M), 2011 WL 1549464, at *1–2 (W.D.N.Y. Apr. 22, 2011) (explaining that if a defendant makes the threshold showing in support of a Franks hearing, discovery may be allowed).[2]

[2] Defendant fails to develop the claim that the Fifth Amendment requires disclosure. The claim is therefore waived. See United States v. Zanino, 895 F.2d 1, 17 (1st Cir. 1990) (issues averted to in a perfunctory manner, unaccompanied by some effort at developed argument, are deemed waived).

III. Analysis

With this law in mind, Defendant moves for the following discovery:

> ***#3-4:*** *The identity of the FLA that seized the computer server hosting Websites 2 and 3 in June 2019, as referenced in ¶¶ 15-16 of the Affidavit.*
>
> ***#8:*** *Any record of the investigative technique(s) utilized by the FLA with respects to the "notification(s)" described in ¶¶ 31-33 of the affidavit.*

[Dkt. No. 80, pp. 17, 20]. The Government has declined to disclose this information. I find that Defendant has failed to show the relevance or materiality of the requested discovery. As an initial matter, Defendant can prosecute a motion to suppress without this discovery. Indeed, review of the sufficiency of the probable cause is limited to the four corners of the affidavit. Aguilar v. Texas, 378 U.S. 108, 109 n.1 (1964), abrogated on other grounds by Illinois v. Gates, 462 U.S. 213 (1983). The seizing FLA is not identified in Moynihan's affidavit; hence, its identity is not relevant to resolution of a motion to suppress.

Defendant nevertheless relies on two exceptions to the purely domestic scope of the exclusionary rule to compel production. "Ordinarily, the Fourth Amendment's exclusionary rule does not apply to foreign searches and seizures, for 'the actions of an American court are unlikely to influence the conduct of foreign police.'" United States v. Valdivia, 680 F.3d 33, 51 (1st Cir. 2012) (quoting United States v. Hensel, 699 F.2d 18, 25 (1st Cir. 1983)). "There are, however, two well-established exceptions to this rule: (1) where the conduct of foreign police shocks the judicial conscience, or (2) where American agents participated in the foreign search, or the foreign officers acted as agents for their American counterparts." Id. (quoting United States v. Mitro, 880 F.2d 1480, 1482 (1st Cir. 1989)). Defendant has failed to proffer any persuasive showing that the first exception applies. Rather, his argument appears to be that if the seizing FLA were identified, the seizing FLA's investigation might be identified, and it may be determined from review of the

investigation that the seizing FLA engaged in conduct which might shock the judicial conscience. This argument is, as it sounds, speculation and in the absence of an offer of proof that the seizure involved conduct that would shock a judicial conscience, fails to meet Defendant's burden.

In suggesting that the 96 IP address information was the product of a joint venture, Defendant assembles information which reflects a history of cooperation and collaboration between U.S. and foreign country law enforcement agencies. [Dkt. No. 80, pp. 4–7]. Defendant also points to the reliance on MLATs between the U.S. and foreign countries to facilitate cooperation in criminal investigations, and notes that adoption of the [redacted] reflects Congress' endorsement of the MLAT between the U.S. and [redacted] to facilitate such cooperation. In the Court's view, a history of collaboration and treaties does not persuade the Court that a joint venture occurred here. Indeed, Moynihan expressly averred that the U.S. did not participate in the investigative work through which the FLA identified the IP address. [Dkt. No. 80-6, ¶ 33]. While Defendant correctly argues that this statement does not preclude the possibility that the U.S. participated in other phases of the investigation, at the same time Defendant offers nothing but this bald assertion of a possibility. Moreover, if U.S. agents had participated in, for instance, the seizure of the websites server(s), common sense suggests that a FLA tip would have been unnecessary to alert agents of the activities of the 96 IP address; rather, U.S. agents would have possessed such information. See Illinois v. Gates, 462 U.S. 213, 238 (1983) (affidavit should be read in a practical, common-sense manner). Lastly, it seems equally unlikely that U.S. agents directed an investigation into what IP addresses accessed the websites, since, as noted in the affidavit, the hidden service websites on the TOR network are accessible globally and users may be located anywhere in the world, not necessarily or only in the U.S.

> ***#6-7:*** *The substance of the notification by the "FLA" to U.S. law enforcement regarding the identification of the IP address in this*

case, as referenced in ¶¶ 31-32 of the affidavit, including but not limited to:

a. the author of the "FLA" notification;
b. the identity of the "U.S. Law Enforcement" agency which received the notification and the recipient;
c. the complete content of the notification, including information on tactics and/or techniques utilized by the "FLA" to determine the identity of the IP address accessing the website;
d. any and all descriptions and/or identifications of Website 2 provided by the "FLA" in its tip to the U.S.;
e. the "further documentation" regarding Websites 2 and 3 provided by the FLA as referenced in ¶¶ 31-32 of the affidavit.

#9: *Any information, document, memorandum, and/or agreement addressing whether the FLA provided the information regarding the IP address in this case as part of a coordinated initiative or program with U.S. law enforcement.*

#16: *Any and all cover sheet(s), correspondence, and/or index list documenting the totality of "tip" and/or "notification" information provided by the FLA.*

[Dkt. No. 80, pp. 18, 20]. The Government produced photocopies of what the Court understands to be some of the communications from the notifying FLA that comprise the substance of the tip about the 96 IP address. These photocopies are heavily redacted, and Moynihan avers that the notifying FLA "provided further documentation naming [Website 2 and Website 3]" by their actual names and as having been accessed by the 96 IP address. [Dkt. No. 80-6, ¶¶ 31–32]. Defendant argues that complete copies of the documents comprising the tip should be produced, in part, to test the truthfulness of Moynihan's averments. [Dkt. No. 80, p. 13]. To support his preliminary discovery burden, Defendant takes issue with how the tip is described in the affidavit—the FLA "notified U.S. law enforcement" that the FLA had determined that at a certain time on a certain date the 96 IP address accessed Websites 2 and 3. Defendant infers that the tip was a single communication and, as such, would be in tension with the fact that there is no single piece of paper which links the 96 IP address to Websites 2 and 3. I disagree. Moynihan's averment summarizes the tip but does not detail how it was communicated. Further, Moynihan expressly averred that in seeking a search warrant, she did not include every fact known to her, but

only the facts she believed were necessary to establish probable cause. [Dkt. No. 80-6, p. 4]. For purposes of Franks discovery, I find that while the tip is drawn from several communications, read together these squarely identify Website 2 and Website 3 as hidden services on the TOR network which supported distribution of child pornography, and as having been accessed by the 96 IP address, and hence that Defendant fails to establish preliminarily a false or recklessly untrue averment. [Dkt. Nos. 80-7 to 80-9]. Defendant also points to a discrepancy between Moynihan's averment that the 96 IP address "accessed" the websites and the Government's statement in discovery that the 96 IP address "accessed or logged into" the websites to suggest a potential false or reckless statement. However, the Government readily conceded at oral argument that it spoke in error by including "logged into." In the Court's view, this argument makes too much of too little. As noted in the caselaw recited above, Defendant is not entitled to Franks discovery without making a substantial preliminary showing.

Defendant also argues that discovery is necessary to allow him to show that the investigation was a joint venture with U.S. law enforcement. [Dkt. No. 80, pp. 16, 19]. For the reasons stated above, I reject this argument.

Finally, I note that insofar as Defendant believes Moynihan's averments fail to link the 96 IP address to the websites, he can make such arguments in support of suppression.

> ***#10:*** *Complete copies of the "advisements" by the FLA to U.S. law enforcement regarding the "independent investigation" and "investigative work through which the FLA identified the IP address information" in this case, as referenced in ¶ 33 of the affidavit.*

[Dkt. No. 80, p. 21]. Having received photocopies of communications comprising the tip, Defendant trains this request on the seizing FLA and the possibility that the seizing FLA engaged in shocks-the-conscience misconduct. Because I find Defendant offers nothing but speculation to support this request, it is denied.

> ***#13:*** *The name of the "Operation," "Task Force," "Initiative," and/or organizing group assigned by the FLA to the investigation in this case, and the name of "Operation," "Task Force," "Initiative," and/or organizing group assigned by the FBI to the investigation in this case, if different.*
>
> ***#14:*** *The specific case FBI ID and/or serial number assigned to the Defendant's case.*

[Dkt. No. 80, pp. 21, 22]. Defendant offers myriad arguments to support production of this information. None of them is persuasive. He argues that the information is relevant to the nature and scope of the investigation and to showing whether there was a joint venture. For the reasons stated above, I find that Defendant has failed to submit a persuasive offer of proof that there was a joint venture here. I also reject the argument that names and numbers assigned to the case are material to defending this case.

Defendant also argues that the information is "necessary to determine whether there were any omissions and/or misstatements" in Moynihan's affidavit. [Dkt. No. 80, p. 21]. This argument ignores the settled law that Defendant must make a substantial preliminary showing for such discovery.

Lastly, Defendant makes the conclusory claim that information responsive to request 14 is Brady material. This claim is undeveloped and summarily rejected.

> ***#15:*** *Any record of action taken in response to the FLA notification by U.S. Law Enforcement agencies, including but not limited to copies of subpoenas and supporting materials (including spreadsheets, charts, lists, and/or other documents) sent to internet service providers, as referenced in ¶¶ 3 and 39 of the affidavit; and copies of returns to such subpoenas.*

[Dkt. No. 80, p. 23]. Insofar as Defendant argues that the Government should produce information regarding steps taken in other investigations in response to notifications from an FLA, such information is neither material nor relevant to Defendant's prosecution and is denied. Defendant further argues that there is a discrepancy between the action taken in this case between the subpoena to Verizon for information associated with the 96 IP address on the date and at the

times identified in the tip and Verizon's response which associates the 96 IP address with Defendant's residence not for only the date and times requested, but for the 10-month period in which the date and times occurred. This discrepancy is not significant. Accordingly, I deny the motion.

> ***#17:*** *With respect to the notification by the FLA to U.S. law enforcement:*
> *a. whether, and how, the FLA determined that the defendant's IP address accessed and/or visited a specific portion of Websites 2 and/or 3, and, if so, what specific portion of Websites 2 and/or 3 was accessed and/or visited;*
> *b. the number of tips provided by the FLA to U.S. law enforcement pursuant to its investigation under the United Kingdom's 2016 Investigatory Powers Act as referenced in its September 16, 2019 letter;*
> *c. the number of websites identified by the FLA to US. law enforcement pursuant to its investigation under the U.K.'s 2016 Investigatory Powers Act;*
> *d. the number of IP addresses identified by the FLA to U.S. law enforcement pursuant to its investigation under the U K. 's 2016 Investigatory Powers Act.*

[Dkt. No. 80, p. 24]. As to item (a), the Government reported that it is not in possession of information showing which portions of Websites 2 and 3 the 96 IP address accessed. Accordingly, the motion is denied as to item (a). As to items (b) through (d), Defendant argues that the responsive information is relevant to the scope of the investigation, and the method and reliability of the identification of the 96 IP address. In the Court's view, for purposes of this instant prosecution, the method and reliability of the identification of the 96 IP address depend on Moynihan's averments set forth in the four corners of her affidavit. Defendant has not made an offer of proof to warrant discovery to challenge in a Franks hearing the veracity of her averments. Defendant is of course free to argue that the averments fail to establish the reliability of the tipster, here the notifying FLA. Insofar as Defendant seeks items (b) through (d) to prove a joint venture, I find he has failed to make a showing to support the discovery requests.

IV. Conclusion

For the reasons stated above, Defendant's Motion to Compel Discovery [Dkt. No. 80] IS DENIED.

October 4, 2021

/s/ David H. Hennessy
David H. Hennessy
United States Magistrate Judge